AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims

1. (Original) A method of processing a message to determine a tag value from the message and from a key according to a message authentication code, the method comprising:

selecting one of a plurality of symbols, the plurality of symbols forming a codeword encoding a data item derived from the message, the codeword encoding the data item according to an error correcting code, wherein said key determines which one of said plurality of symbols is selected; and

determining the tag value to be the selected symbol.

2. (Original) A method according to claim 1, wherein the data item derived from the message consists of said message.

3. (Original) A method according to claim 1, further comprising determining said data item to be a hash value of a one-way hash function calculated from the message.

4. (Original) A method according to claim 1, wherein the key is short enough to be communicated via a user interaction.

5. (Original) A method according to claim 1, wherein the error correcting code is a Reed-Solomon code and wherein the tag value is determined by evaluating a Reed-Solomon encoding polynomial at a point determined by the key.

6. (Original) A method according to claim 1, wherein the tag value is an element in a finite field.

7. (Original) A method according to claim 1, further comprising communicating at least a contribution to the message from a sender to a receiver via a first communications channel; and communicating the tag value and/or the key from the sender to the receiver via a second communications channel different from the first communications channel.

8. (Original) A method according to claim 7, wherein the second communications channel includes a user interaction.

9. (Currently Amended) A communications device for communicating data messages, the communications device comprising:

processing means that is adapted to determine a tag value from a message and from a key according to a message authentication code, and wherein the processing means is further adapted to select one of a plurality of symbols, the plurality of symbols forming a codeword encoding a data item derived from the message, the codeword encoding the data item according to an error correcting code, wherein said key determines which one of said plurality of symbols is selected, and wherein the processing means is further adapted to determine the tag value to be the selected symbol.

10. (Currently Amended) A computer program product ~~configured~~ *embodied* on a computer readable medium adapted to configure a processor to process a message to determine a tag value from the message and from a key according to a message authentication code, the computer program product comprising:

a computer readable storage medium having computer readable program code embodied therein, the computer readable program code further comprising:

computer readable program code ~~for selecting~~ adapted to configure the processor to select one of a plurality of symbols, the plurality of symbols forming a

codeword encoding a data item derived from the message, the codeword encoding the data item according to an error correcting code, wherein said key determines which one of said plurality of symbols is selected; and

computer readable program code ~~for determining~~ adapted to configure the processor to determine the tag value to be the selected symbol.

11. (Currently Amended) A computer program product ~~configured~~ embodied on a computer readable medium adapted to configure a processor to ~~communicating~~ communicate data messages, the computer program product comprising:

a computer readable storage medium having computer readable program code embodied therein, the computer readable program code further comprising:

computer readable program code ~~for determining~~ adapted to configure the processor to determine a tag value from a message and from a key according to a message authentication code;

computer readable program code ~~for selecting~~ adapted to configure the processor to select one of a plurality of symbols, the plurality of symbols forming a codeword encoding a data item derived from the message, the codeword encoding the data item according to an error correcting code, wherein said key determines which one of said plurality of symbols is selected; and

computer readable program code ~~for determining~~ adapted to configure the processor to determine the tag value to be the selected symbol.

12. (Original) A communications device for communicating data messages, the communications device comprising:

a processing unit that is adapted to determine a tag value from a message and from a key according to a message authentication code, and wherein the processing unit is adapted to select one of a plurality of symbols, the plurality of symbols forming a codeword encoding a data item derived from the message, the codeword encoding the data item according to an error correcting code, wherein said key determines which one of said plurality of symbols is selected, and wherein the processing unit is adapted to determine the tag value to be the selected symbol.